CLAIMS

What is claimed is:

1.   A method performed by a user terminal of a wireless access network, the method comprising:

obtaining a time reference from an access point of the wireless access network;

receiving a digital certificate issued by a certificate authority from the access point, the digital certificate having a validity period;

requesting certification of the time reference by a trusted entity;

receiving certification of the time reference; and

validating the digital certificate.

2.   The method of claim 1, wherein requesting certification of the time reference comprises sending a message used to authenticate the user terminal to the access point, the message containing a timestamp based on the time reference and an identification of the trusted entity by which certification is to be performed.

3.   The method of claim 2, wherein the message contains a list of trusted entities by which certification may be performed.

4.   The method of claim 2, wherein receiving certification of the time reference comprises receiving a message from the access point, the message being signed by the trusted entity and containing information to verify the timestamp.

5.   The method of claim 1, wherein requesting certification of the time reference comprises sending a message to the trusted entity, the message containing a timestamp and a request to compare the timestamp to a local time of the trusted entity.

6.   The method of claim 1, wherein validating the access point comprises determining whether the validity period has expired using the certified time reference.

7.   The method of claim 1, wherein the time reference comprises an absolute frame number.

8.   A user terminal comprising:

a clock to maintain a time reference obtained from an access point;

a transmitter to send a request for certification of the time reference by a trusted entity;

a receiver to receive the certification of the time reference and a digital certificate issued by a certificate authority from the access point, the digital certificate having a validity period; and

a processor coupled to the receiver to validate the digital certificate.

9.   The user terminal of claim 8, wherein the user terminal requests certification of the time reference by sending a message used to authenticate the user terminal to the access point, the message containing a timestamp based on the time reference maintained by the clock and an identification of the trusted entity by which certification is to be performed.

10.   The user terminal of claim 9, wherein the message contains a list of trusted entities by which certification may be performed.

11.   The user terminal of claim 9, wherein the user terminal receives the certification of the time reference by receiving a message from the access point, the message being signed by the trusted entity and containing information to verify the timestamp.

12.   The user terminal of claim 8, wherein the user terminal requests certification of the time reference by sending a message to the trusted entity, the message containing a timestamp based on the time reference maintained by the clock and a request to compare the timestamp to a local time of the trusted entity.

13.   The user terminal of claim 8, wherein the user terminal validates the access point by determining whether the validity period has expired using the certified time reference.

14.   The user terminal of claim 8, wherein the time reference comprises an absolute frame number.

15.   A method performed by an access point of a wireless access network, the method comprising:

        receiving a message including a timestamp from a user terminal of the wireless access network;

        authenticating the user terminal using the message;

        sending a request for certification of the timestamp to a trusted entity that is trusted by the user terminal;

receiving a time certification message signed by the trusted entity including a verification of the timestamp; and

sending the time certification message to the user terminal.

16. The method of claim 15, wherein the message further includes a request that the timestamp be certified by the trusted entity and an identification of the trusted entity.

17. The method of claim 16, wherein the identification of the trusted entity comprises a list of entities trusted by the user terminal.

18. The method of claim 15, wherein sending a request for certification of the timestamp comprises forwarding the timestamp to the trusted entity so that the trusted entity can compare the timestamp to a local time of the trusted entity.

19. An access point comprising:

a receiver to receive a message including a timestamp from a user terminal;

a processor coupled to the receiver to authenticate the user terminal based on the received message; and

a transmitter coupled to the processor, to send a request for certification of the timestamp to a trusted entity that is trusted by the user terminal, and to forward a certification message received from and signed by the trusted entity, the certification message including a verification of the timestamp.

20. The access point of claim 19, wherein the received message further includes a request that the timestamp be certified by the trusted entity and an identification of the trusted entity.

21. The access point of claim 20, wherein the identification of the trusted entity comprises a list of entities trusted by the user terminal.

22. The access point of claim 19, wherein the transmitter further forwards the timestamp to the trusted entity so that the trusted entity can compare the timestamp to a local time of the trusted entity.

23. A machine-readable medium storing data representing instructions that, when executed by a processor of a user terminal, cause the processor to perform operations comprising:

obtaining a time reference from an access point;

receiving a digital certificate issued by a certificate authority from the access point, the digital certificate having a validity period;

requesting certification of the time reference by a trusted entity;

receiving certification of the time reference; and

validating the digital certificate.

24. The machine-readable medium of claim 23, wherein requesting certification of the time reference comprises sending a message used to authenticate the user terminal to the access point, the message containing a timestamp based on the time reference and an identification of the trusted entity by which certification is to be performed.

25. The machine-readable medium of claim 24, wherein the message contains a list of trusted entities by which certification may be performed.

26. The machine-readable medium of claim 24, wherein receiving certification of the time reference comprises receiving a message from the access point, the message being signed by the trusted entity and containing information to verify the timestamp.

27. The machine-readable medium of claim 23, wherein requesting certification of the time reference comprises sending a message to the trusted entity, the message containing a timestamp and a request to compare the timestamp to a local time of the trusted entity.

28. The machine-readable medium of claim 23, wherein validating the access point comprises determining whether the validity period has expired using the certified time reference.

29. The machine-readable medium of claim 23, wherein the time reference comprises an absolute frame number.

30. A machine-readable medium storing data representing instructions that, when executed by a processor of an access point, cause the processor to perform operations comprising:

receiving a message including a timestamp from a user terminal;

authenticating the user terminal using the message;

sending a request for certification of the timestamp to a trusted entity that is trusted by the user terminal;

receiving a time certification message signed by the trusted entity including a verification of the timestamp; and

sending the time certification message to the user terminal.

I:\ArrayComm\P206 - i-TAP Time Certification\P206 Application.doc

31.   The machine-readable medium of claim 30, wherein the message further includes a request that the timestamp be certified by the trusted entity and an identification of the trusted entity.

32.   The machine-readable medium of claim 31, wherein the identification of the trusted entity comprises a list of entities trusted by the user terminal.

33.   The machine-readable medium of claim 30, wherein sending a request for certification of the timestamp comprises forwarding the timestamp to the trusted entity so that the trusted entity can compare the timestamp to a local time of the trusted entity.